M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Gregory Haroutunian (SBN 330263)
gharoutunian@justice4you.com
**CLAYEO C. ARNOLD,**
**A PROFESSIONAL LAW CORP.**
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916)239-4778
Fax: (916) 924-1829

TERENCE R. COATES (*pro hac vice forthcoming*)
tcoates@msdlegal.com
JUSTIN C. WALKER (*pro hac vice forthcoming*)
jwalker@msdlegal.com
DYLAN J. GOULD (*pro hac vice forthcoming*)
dgould@msdlegal.com
**MARKOVITS, STOCK & DEMARCO, LLC**
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219

*Attorney for Plaintiffs and the Proposed Class*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION**

| | |
|---|---|
| STEVEN PRYOR, individually, and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>vs.<br><br>BLACKHAWK NETWORK, INC., dba BLACKHAWK ENGAGEMENT SOLUTIONS,<br><br>Defendant. | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>DEMAND FOR JURY TRIAL |

Plaintiff Steven Pryor, individually, and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendant Blackhawk Network, Inc. d/b/a Blackhawk

Engagement Solutions ("Blackhawk"" or "Defendant"), a California corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations on information and belief, except as to his own actions, which are made on personal knowledge, the investigation of his counsel, and the facts that are a matter of public record.

## I. NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Blackhawk Network, Inc., which offers branded payment programs, including prepaid gift cards, to customers.

2. Blackhawk Network, Inc. is headquartered in Pleasanton, California.

3. Blackhawk acts as a third-party service provider on behalf of Pathward N.A. ("Pathward"). Pathward uses Blackhawk to activate and manage certain prepaid incentive cards referred to as Pathward Prepaid Cards ("Prepaid Card" or "Prepaid Cards").

4. Blackhawk operates the website www.MyPrepaidCenter.com ("MyPrepaidCenter.com") on behalf of Gift Card holders to activate and manage Pathward's Prepaid Cards. To purchase and use Prepaid Cards, Plaintiff and Class Members were required to provide certain sensitive, non-public information to Defendant by entering this information on MyPrepaidCenter.com.

5. Unfortunately, Blackhawk failed to properly secure and safeguard the personally identifiable information provided by customers, including Plaintiff and Class Members, that appeared on the MyPrepaidCenter.com profile, including, without limitation, their unencrypted and unredacted first and last names, email addresses, phone numbers ("PII"), their payment card data in combination with information "related to the Prepaid Card profiles," which included, but was not limited to, information added by customers to PrepaidCenter.com, such as card numbers, expiration dates, and CVV security

codes ("PCD") and other sensitive information (collectively with PII and PCD, "Private Information").[1]

6. On information and belief, this Data Breach was engineered and targeted at accessing and exfiltrating the Private Information of Plaintiff and Class Members in order for criminals to use that information in furtherance of theft, identity crimes, and fraud.

7. Defendant's failure to prevent and detect the Data Breach is particularly egregious considering the nature of its business and the Private Information it collected, the myriad data breaches all over the country, and its own experience with a substantially similar data breach described in more detail below. The aggregate information acquired by cybercriminals in this Data Breach is particularly concerning considering that Defendant's customers provided Private Information, which can be used to commit fraud against Plaintiff and Class Members as well as steal their identities.

8. Plaintiff brings this class action against Blackhawk to seek damages for himself and other similarly situated consumers impacted by the Data Breach ("Class Members"), as well as other equitable relief, including, without limitation, injunctive relief designed to protect the sensitive information of Plaintiff and other Class Members from further data breach incidents.

9. On October 31, 2022, Blackhawk filed a Notice of Data Breach ("Notice") with the Attorney General of Montana. The Notice states, on September 11, 2022, Blackhawk "discovered irregular activity in connection" with MyPrepaidCenter.com.[2] Blackhawk claims it "took prompt steps to investigate the incident, and we stopped the irregular activity on September 12, 2022."[3] In addition, Blackhawk states the "unauthorized acquisition occurred between September 4-12, 2022."[4] The Notice provided to the Montana Attorney General is as follows:

---

[1] *Blackhawk Network Notice of Data Breach*, Oct. 31, 2022, archived by the Montana Attorney General, *available at*: https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-675.pdf (last accessed Nov. 8, 2022).
[2] *Id.*
[3] *Id.*
[4] *Id.*

**What Happened?**

On September 11, 2022, we discovered irregular activity in connection with www.MyPrepaidCenter.com, the website that Blackhawk operates for cardholders to activate and manage Pathward Prepaid Cards. We took prompt steps to investigate the incident, and we stopped the irregular activity on September 12, 2022. Our investigation revealed that the irregular activity involved unauthorized acquisition of information about you described below. The unauthorized acquisition occurred between September 4–12, 2022.

**What Information Was Involved?**

This incident involved information you provided for your www.MyPrepaidCenter.com profile, including your first and last name, email address, and phone number (if any). It also included information relating to your Pathward Prepaid Card(s) you added to your www.MyPrepaidCenter.com profile, such as card numbers, expiration dates, and CVV codes.

10. Also, on October 31, 2022, through its attorney Pathward filed a similar Notice of Data Breach ("Pathward Notice") with the Attorney General of Iowa. The Notice, dated September 11, 2022, states that Blackhawk "discovered irregular activity in connection" with MyPrepaidCenter.com.[5]

11. As a result of Defendant's failure to prevent the Data Breach, or detect it during its occurrence thousands of MyPrepaidCenter.com customers across the United States are suffering and will continue to suffer real and imminent harm as a direct consequence of Defendant's conduct, which includes: (a) refusing to take adequate and reasonable measures to ensure its data systems were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to adequately audit and monitor its third party data security vendors; (d) failing to disclose to its customers the material fact that it or its vendors did not have adequate computer systems and security practices to safeguard customers' personal and financial information; and (e) failing to provide timely and adequate notice of the data breach.

12. The injuries suffered by Plaintiff and Class Members as a direct result of the Data Breach

[5] *Pathward, N.A. Data Security Incident*, archived by the Iowa Attorney General, *available at*: https://www.iowaattorneygeneral.gov/media/cms/10312022_Blackhawk_Engagement_Solut_1D9CB60967722.pdf (last accessed Nov. 8, 2022).

include, *inter alia*:

a. Unauthorized charges on their payment card accounts;

b. Theft of their personal and financial information;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. Loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

f. The present and continuing injury flowing from potential theft, fraud, and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted to Blackhawk for the sole purpose of using Blackhawk's services and with the mutual understanding that Blackhawk would safeguard Plaintiff's and Class Members' Private Information against theft and not allow access to and misuse of their information by others;

h. Money paid to Blackhawk during the period of the Data Breach in that Plaintiff and Class Members would not have used Blackhawk's services or products, or would have paid less for their services or products, had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Private Information and had Plaintiff and Class Members known that Blackhawk would not provide timely and accurate notice of the Data Breach; and,

i. Continued risk to their PII and PCD, which remains in the possession of Blackhawk and its vendors, and which is subject to further breaches so long as Blackhawk continues to fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data in its possession.

13. Examples of the harms experienced by Blackhawk customers as a direct and foreseeable consequence of its conduct include the experiences of the representative Plaintiff described below.

## II. THE PARTIES

***Plaintiff Steven Pryor***

14. Plaintiff Steven Pryor is a citizen of the State of Colorado and a is a resident of Johnston, Colorado. Plaintiff is the owner of two payment cards registered on MyPrepaidCenter.com.

***Defendant Blackhawk***

15. Defendant is a privately held corporation incorporated in the State of California. Defendant's headquarters is located at 6220 Stoneridge Mall Road, Pleasanton, California 94588. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

## III. JURISDICTION AND VENUE

16. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C.

§1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

17. This Court has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in California and this District through its headquarters, offices, parents, and affiliates.

18. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

## IV. FACTUAL ALLEGATIONS

***Background***

19. Blackhawk is primarily engaged in providing "global branded payments" to its customers located within the United States and abroad, which includes gift cards, prepaid incentive cards, other online payment options for employers and merchants, gaming, and gambling options.[6] Blackhawk is a privately held company with corporate headquarters in Pleasanton, California.

20. Blackhawk operates a consumer facing website located at www.blackhawknetwork.com ("Blackhawknetwork.com"). Customers or potential customers can then access MyPrepaidCenter.com through Blackhawknetwork.com.

21. To make a purchase on MyPrepaidCenter.com a customer must provide certain PII and PCD, specified in Blackhawk Network Privacy Notice ("Privacy Notice") that the policy pertains to all visitors, customers, users of apps, and users of gift card and banded payments. Specifically, the Private Information, which Defendant collects, includes, but is not limited to:

[6] Blackhawk Network Website, *available at*: https://blackhawknetwork.com/ (last accessed on Nov. 8, 2022).

- Contact information, such as name, email address, mailing address, fax, or phone number;
- Payment and financial information, such as credit or other payment card information, bank account, or billing address;
- Shipping address and related details;
- Resume, employment and education history, name and contact details, background details, and references when you apply to job postings or contact us about employment opportunities;
- Company and employment information;
- Subject to applicable local law restrictions, Social Security number or other national tax ID number (for clients and potential clients);
- Unique identifiers such as username, account number, or password;
- Preference information such as product wish lists, order history, or marketing preferences;
- Information about businesses, such as company name, size, or business type; and
- Demographic information, such as age, gender, interests and ZIP or postal code.[7]

22. Defendant also specifies in the Privacy Policy that it acts as the "Controller" of the Private Information supplied.

23. When they provided their Private Information to Defendant, Plaintiff and Class Members relied on Defendant (a large, sophisticated internet retailer) to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

[7] *Blackhawk Network Privacy Notice*, quoting, "Personal Information we Collect" *available at*: https://blackhawknetwork.com/privacy-policy (last accessed on Nov. 8, 2022).

24. Defendant had a duty to take reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to unauthorized third parties. This duty is inherent in the nature of the exchange of the highly sensitive PII and PCD at issue here, particularly where digital transactions are involved.

25. Defendant also recognized and voluntarily adopted additional duties to protect PII and PCD in its Privacy Policy which has been publicly posted to the internet.[8] In its Privacy Policy, Defendant also says the way it uses Private Information is at "the core of our obligations," that it will "not sell" information, and that it will use the information for "our own legitimate and lawful business interests."[9]

26. Despite these duties and promises, Defendant allowed data thieves to infect and infiltrate its MyPrepaidCenter.com website and steal the Private Information of thousands of its customers.

***The Data Breach was foreseeable***

27. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[10]

28. In light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by

---

[8] *Id.*

[9] *Id.*

[10] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/#:~:text=The%20number%20of%20reported%20data%20breaches%20jumped%2068%20percent%20last,of%201%2C506%20set%20in%202017. (last accessed Nov. 8, 2022).

cybercriminals.

29. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

30. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties to keep Private Information confidential and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and the Class from being compromised.

***The Data Breach***

31. On or about October 31, 2022, Defendant notified various state Attorneys General, as well as Plaintiff and Class Members, that, on September 12, 2022, Defendant discovered that MyPrepaidCenter.com experienced "irregular activity."[11]

32. The Notice informed Plaintiff and Class Members that "Our investigation revealed that irregular activity involved the unauthorized acquisition of information about you." This information included first and last name, email address, and phone numbers, but it also included information relating to the Pathward Prepaid Card(s), added on the MyPrepaidCenter.com profile such as card numbers, expiration dates, and CVV security codes.[12]

33. The Private Information exfiltrated in the Data Breach was unencrypted and captured

[11] *Blackhawk Network Notice of Data Breach*, Oct. 31, 2022, archived by the Iowa Attorney General, *available at*: https://www.iowaattorneygeneral.gov/media/cms/10312022_Blackhawk_Engagement_Solut_1D9CB60967722.pdf (last accessed Nov. 8, 2022).

[12] *Id.*

directly from MyPrepaidCenter.com.[13]

34. Defendant claims it "blocked your impacted Pathward Prepaid Card(s)," yet it remained silent about what happened to the stolen Personal Information.[14]

35. Despite Defendant's promises that it: (i) would not disclose consumers' Private Information to unauthorized third parties; and (ii) would protect consumers' Private Information with adequate security measures, it appears that Defendant did not even implement, or require its third-party vendors to implement, basic security measures such as immediately encrypting PCD.

***Blackhawk Experienced a Substantially Similar Data Breach Two Years Earlier***

36. According to an earlier Security Incident Notification ("Notification"), on August 8, 2020, Blackhawk "detected some activity on its website GiftCards.com, indicating a possible 'brute force attack.'"[15]

37. Blackhawk conducted an investigation on August 14, 2020 and determined that the incident resulted in "unauthorized access" to a number of accounts.[16]

38. The Notification also indicates similar Private Information was taken in the 2020 data breach as was taken in the Data Breach that is the subject of this class action:

> For any account accessed, the perpetrator(s) would have only had access to the customer's transaction history, original balance information for gift card(s), and account profile information, which includes customer name, email address, postal address, the name and contact information of any gift card recipient(s), and the last four digits of the credit card used in prior transactions. The perpetrator(s) would not have been able to access the full numbers of any gift cards purchased or the credit cards used to purchase gift cards through

---

[13] *Id.*

[14] *Id.*

[15] *Blackhawk Security Incident Notification*, August 28, 2020, archived at the Maryland Attorney General, *available at:* https://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2020/itu-331656.pdf (last accessed on Nov. 8, 2022).

[16] *Id.*

customer accounts. Further, the perpetrator(s) would not have been able to initiate a transaction using any stored cards without the Card Identification Number (CID) code for the particular credit card (which would not have been accessible through GiftCard.com).[17]

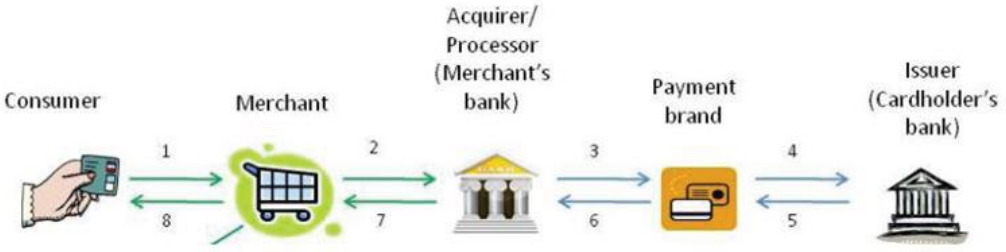
***Securing PII and Preventing Breaches***

39. Given Blackhawk's recent experience with data breaches, it should have been even more aware and taken further precautions to secure PII and other private information.

40. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to an e-commerce retailer (through an e-commerce website) to pay for merchandise. The card is then "swiped," and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (*i.e.*, the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (*i.e.*, cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction. See graphic below:[18]

[17] *Id.*

[18] *Payments 101: Credit and Debit Card Payments*, FIRST DATA, at 7 (Oct. 2010), http://euro.ecom.cmu.edu/resources/elibrary/epay/Payments-101.pdf (last accessed on Nov. 8, 2022).




| | |
|---|---|
| 1 | The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website. |
| 2 | The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer. |
| 3 | The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor |
| 4 | The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction. |
| 5 | If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf. |
| 6 | The card brand forwards the authorization code back to the acquirer/processor. |
| 7 | The acquirer/processor sends the authorization code back to the merchant. |
| 8 | The merchant concludes the sale with the customer. |

41. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

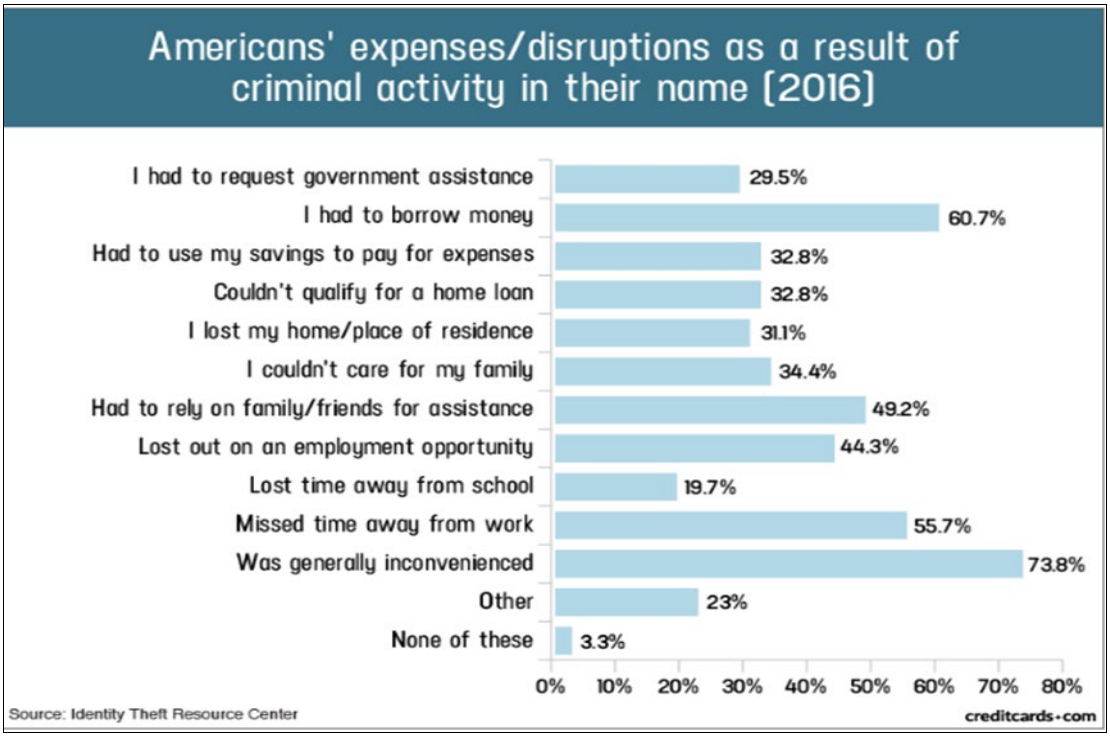
42. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment it is "swiped," hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the cardholder's personal information stored in the retailer's computers.

43. The financial fraud suffered by Plaintiff and other customers demonstrates that Defendant , and/or its third party vendors, chose not to invest in the technology to encrypt payment card data (PCD)

at point-of-sale to make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or failed to provide sufficient control of employee credentials and access to computer systems to prevent a security breach and/or theft of PCD.

44. These failures demonstrate a clear breach of the Payment Card Industry Data Security Standards (PCI DSS), which are industry-wide standards for any organization that handles PCD.

45. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Private Information:[19]




46. Plaintiff and Class Members have experienced one or more of these harms as a result of the data breach.

[19] Jason Steele, *Credit Card Fraud and ID Theft Statistics,* CREDITCARDS.COM (June 11, 2021), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited October 27, 2020) [https://web.archive.org/web/20200918073034/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/].

47. Furthermore, theft of Private Information is also gravely serious. Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

48. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

49. Private Information and PCD are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

50. There is a strong probability that entire batches of stolen payment card information have been dumped on the black market or are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

51. Plaintiff and Class Members have and will continue to suffer injuries as a direct result of the Data Breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

[20] U.S. Gov't Accountability Off., GAO 07737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed on Nov. 8, 2022).

a. Finding fraudulent charges;
b. Canceling and reissuing cards;
c. Purchasing credit monitoring and identity theft prevention;
d. Addressing their inability to withdraw funds linked to compromised accounts;
e. Removing withdrawal and purchase limits on compromised accounts;
f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;
h. Resetting automatic billing instructions; and
i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

52. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

53. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

54. As a direct and proximate result of the Data Breach, Plaintiff's PII and PCD was "skimmed" and exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the fraud perpetrated against Plaintiff and Class Members.

55. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an immediate and continuing increased risk of harm from fraud. Plaintiff and Class Members now have to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing, or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

56. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly

related to the Data Breach.

57. Plaintiff and Class Members also suffered a loss of value of their PII and PCD when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

58. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Plaintiff and Defendant included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiff and the Class Members did not get what they paid for.

59. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

60. Plaintiff and Class Members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including PII and PCD;

b. Improper disclosure of their PII and PCD property;

c. The present and continuing injury flowing from potential fraud and identity theft posed by customers' Private Information being placed in the hands of criminals;

d. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' Private Information for which there is a well-established and quantifiable national and

international market; and,

h. The loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

61. The substantial delay in providing notice of the Data Breach deprived Plaintiff and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members was and has been driven even higher.

***Value of Personal Identifiable Information***

62. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

63. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[23] In fact, the data marketplace is so

[21] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed on Nov. 8, 2022).

[22] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed on Nov. 8, 2022).

[23] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed on Nov. 8, 2022).

sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[24] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[25]

64. As a result of the Data Breach, Plaintiff's, and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is likely readily available to others, and the rarity of the Private Information has been destroyed, thereby causing additional loss of value.

65. The fraudulent activity resulting from the Data Breach may not come to light for years and Plaintiff and Class Members face a lifetime risk of fraud and identity theft as a result of the Data Breach.

66. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

[24] See Data Coup, https://datacoup.com/ (last accessed on Nov. 8, 2022).

[25] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Nov. 8, 2022).

[26] U.S. Gov't Accountability Off., GAO 07737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed on Nov. 8, 2022).

67. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, particularly given the sensitive nature of their purchases, and of the foreseeable consequences that would occur if Defendant's data security system was breached (as it had been as recently as 2020), including, specifically, the significant costs and risks that would be imposed on Plaintiff and Class Members as a result of a breach.

68. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

69. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's storage platform, amounting to tens or hundreds of thousands of individual's detailed, Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

70. To date, Defendant has offered no credit monitoring or identity theft services. It has only offered to provide a replacement Pathway Prepaid Card(s). This is wholly inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here.

71. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures, and failure to adequately investigate, monitor, and audit its third-party vendors, to protect the Private Information of Plaintiff and Class Members.

**A. PLAINTIFF PRYOR'S EXPERIENCE**

72. Plaintiff suffered actual injury from having his Private Information compromised and/or stolen as a result of the Data Breach.

73. Plaintiff suffered actual injury and damages in paying money to and using services from Defendant during the Data Breach that he would not have paid or ordered had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendant provided timely and accurate notice of the Data Breach.

74. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his personal and financial information – a form of intangible property that the Plaintiff entrusted to Defendant for the purpose of making purchases on its website and which was compromised in, and as a result of, the Data Breach.

75. Plaintiff suffers present and continuing injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

76. Plaintiff has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected, and safeguarded from future breaches.

77. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff has spent several hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

78. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity crimes, fraud, and theft. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

79. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

80. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

## V. CLASS ACTION ALLEGATIONS

81. Plaintiff brings this nationwide class action on behalf of himself, and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

82. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all persons who were sent a notice of the Data Breach.**

83. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and Members of their staff.

84. Plaintiff reserves the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

85. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on

information and belief, the Class consists of at least 165,727[27] current and former customers of Defendant whose sensitive data was compromised in Data Breach.

86. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their PII and PCD;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

[27] See *Blackhawk Network Notice of Data Breach*, Oct. 31, 2022, archived by the Iowa Attorney General, *available at*: https://www.iowaattorneygeneral.gov/media/cms/10312022_Blackhawk_Engagement_Solut_1D9CB60967722.pdf (last accessed Nov. 8, 2022).

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breach implied or express contracts with Plaintiff and Class Members;

m. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

o. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

87. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

88. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class and has no interests antagonistic to those of other Class Members. Plaintiff's counsel are competent and experienced in litigating Class actions.

89. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

90. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

91. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

**COUNT I**
**Negligence**
**(On behalf of Plaintiff and Class Members)**

92. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 92.

93. Defendant solicited and gathered the Private Information, including the PCD, of Plaintiff and Class Members to facilitate sales transactions.

94. Defendant knew, or should have known, of the risks inherent in collecting the PII and PCD of Plaintiff and the Class Members and the importance of adequate security. Defendant also knew about numerous, well-publicized payment card data breaches involving other national retailers, including its own similar data breach from two years ago.

95. Defendant owed duties of care to Plaintiff and the Class Members whose Private Information was entrusted to it. Defendant's duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To exercise reasonable care in selecting its third-party vendors and monitoring and auditing their data security practices ensuring compliance with legal and industry standards and obligations;

c. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the PCI DSS and consistent with industry-standard practices;

d. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

e. To promptly notify Plaintiff and Class Members of the data breach.

96. By collecting this data and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property, to prevent disclosure of Private Information, and to safeguard the Private Information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in case of a data breach.

97. Defendant's duty of care extended to ensuring that any third-party vendors it hired and that had exposure to the Private Information of Plaintiff and Class Members would implement adequate measures to prevent and detect cyber intrusions.

98. Because Defendant knew that a breach of its systems would damage thousands of its customers, including Plaintiff and Class Members, it had a duty to adequately protect their Private Information.

99. Defendant owed a duty of care not to subject Plaintiff and the Class Members to an unreasonable risk of harm because they were the foreseeable and probable victims of any inadequate security practices.

100. Defendant had a duty to implement, maintain, and ensure reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Private Information.

101. Defendant knew, or should have known, that its computer systems and security practices did not adequately safeguard the Private Information of Plaintiff and the Class Members.

102. Defendant knew, or should have known, that the computer systems and security practices of its third-party vendors did not adequately safeguard the Private Information of Plaintiff and the Class Members.

103. Defendant breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and the Class Members.

104. Defendant breached its duties of care by failing to provide prompt notice of the data breach to the persons whose PII and PCD was compromised.

105. Defendant acted with reckless disregard for the security of the Private Information of Plaintiff and the Class Members because Defendant knew or should have known that its computer systems and data security practices, and those of its third-party vendors, were not adequate to safeguard the PII and PCD that that it collected, which hackers targeted in the Data Breach.

106. Defendant acted with reckless disregard for the rights of Plaintiff and the Class Members by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use the Private Information compromised in the data breach.

107. Defendant had a special relationship with Plaintiff and the Class Members. Plaintiff's and the Class Members' willingness to entrust Defendant with their Private Information was predicated on the mutual understanding that Ruger would implement adequate security precautions. Moreover, Defendant was in an exclusive position to protect its systems (and the Private Information) from attack. Plaintiff and Class Members relied on Defendant to protect their Private Information.

108. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII and PCD. Defendant's misconduct included failing to:

a. Secure its e-commerce website;

b. Secure access to its and its vendors' servers;

c. Audit and monitor its vendors;

d. Comply with industry standard security practices;

e. Follow the PCI-DSS standards;

f. Encrypt PCD at the point-of-sale and during transit;

g. Employ adequate network segmentation;

h. Implement adequate system and event monitoring;

i. Utilize modern payment systems that provided more security against intrusion;

j. Install updates and patches in a timely manner; and

k. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

109. Defendant also had independent duties under the FTC Act and state laws that required it to reasonably safeguard Plaintiff's and the Class Members' PII and PCD and promptly notify them about the data breach.

110. Defendant breached the duties it owed to Plaintiff and Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols, and practices sufficient to protect their PII and PCD both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the Data Breach, and

d. By failing to timely and accurately disclose that the PII and PCD of Plaintiff and the Class had been improperly acquired or accessed.

111. But for Defendant's wrongful and negligent breach of the duties it owed Plaintiff and the Class Members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

112. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class Members have suffered damages and are at imminent risk of further harm.

113. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was reasonably foreseeable.

114. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct.

115. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT II**
**Breach of Implied Contract**
**(On behalf of Plaintiff and Class Members)**

116. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 115.

117. When Plaintiff and Class Members provided their PII and PCD to Defendant in making purchases on its website, they entered into implied contracts under which Defendant agreed to protect their PII and PCD and timely notify them in the event of a data breach.

118. Defendant invited its customers, including Plaintiff and the Class, to make purchases of Prepaid Gift cards on its website using payment cards in order to increase sales by making purchases more convenient.

119. An implicit part of the offer was that Defendant would safeguard their Private Information using reasonable or industry-standard means and would timely notify Plaintiff and the Class in the event of a data breach.

120. Defendant also affirmatively represented in its Privacy Policy that it protected the Private Information of Plaintiff and the Class in several ways, as described above.

121. Based on the implicit understanding and also on Defendant's representations, Plaintiff and the Class accepted the offers and provided Defendant with their PII and PCD by using their payment cards in connection with purchases on the Defendant website during the period of the data breach.

122. Defendant manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiff's and Class Members' PII and PCD through, among other things, its Privacy Notice.

123. Defendant further demonstrated an intent to safeguard the Private Information of Plaintiff and Class Members through its conduct. No reasonable person would provide sensitive, non-public information to a retailer without the implicit understanding that the retailer would maintain that information as confidential.

124. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

125. Plaintiff and Class Members would not have provided their PII and PCD to Defendant had they known that Defendant would not safeguard their PII and PCD as promised or provide timely notice of a data breach.

126. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

127. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' Private Information and failing to provide them with timely and accurate notice when their Private Information was compromised in the Data Breach.

128. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breaches of its implied contracts with them.

**COUNT III**
**Unjust Enrichment**
**(on behalf of Plaintiff and Class Members)**

129. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 115.

130. This claim is brought in the alternative to Plaintiff's claim for breach of implied contract.

131. Defendant funds its data security measures entirely from its general revenue, including payments made by Plaintiff and Class Members.

132. As such, a portion of the payments made by Plaintiff and Class Members was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

133. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods (Prepaid Gift Cards, specifically) and services from Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should

have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

134. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

135. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information and instead directing those funds to its own profit. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

136. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

137. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

138. Plaintiff and the Class have no adequate remedy at law.

139. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members of the Class conferred on it.

140. Defendant should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiff and Class Members proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and the Class overpaid, plus attorneys' fees, costs, and interest thereon.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

B. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing one of the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the Classes requested herein;

C. Judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper;

D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

E. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

F. A judgment in favor of Plaintiff and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

G. An award of such other and further relief as this Court may deem just and proper.

## JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Date: November 11, 2022

Respectfully Submitted,

*/s/ M. Anderson Berry*

M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Gregory Haroutunian (SBN 330263)
gharoutunian@justice4you.com
**CLAYEO C. ARNOLD,**
**A PROFESSIONAL LAW CORP.**

865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829

TERENCE R. COATES (*pro hac vice forthcoming*)
tcoates@msdlegal.com
JUSTIN C. WALKER (*pro hac vice forthcoming*)
jwalker@msdlegal.com
DYLAN J. GOULD (*pro hac vice forthcoming*)
dgould@msdlegal.com
**MARKOVITS, STOCK & DEMARCO, LLC**
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219

*Attorneys for Plaintiffs and the Proposed Classes*